基于小波变换去噪的相关功耗分析攻击研究与实现

段晓毅，陈　东，高献伟，范晓红，靳济方
(北京电子科技学院 电子信息工程系，北京 100070)

摘　要：为了提高功耗分析攻击效率，减少噪声影响，研究了小波变换去噪对功耗攻击的影响以及相关功耗分析攻击（correlation power analysis，CPA）的相关系数与攻击效果的关系，提出使用平移不变量小波法与小波模极大值法对功耗曲线进行去噪预处理，该方法使用卡尔曼滤波法、小波模极大值法与平移不变量小波法对功耗曲线进行去噪预处理，再对原始数据及去噪后数据分别进行 CPA。实验结果显示，与原始数据相比，使用平移不变量小波法改进的 CPA 相关系数比仅使用 CPA 分析提高了 165%，比卡尔曼滤波法提高 31.4%，比小波模极大值法相关系数据提高 26.4%，同时攻击成功所需要的功耗曲线减少了 92%。实验结果表明的使用平移不变量小波法改进的相关功耗分析攻击效果最好。

关键词：能量攻击；平移不变量小波法；相关功耗；密码芯片
中图分类号：TP309.2　　doi: 10.19734/j.issn.1001-3695.2018.09.0757

Research and implementation of correlation power analysis based on Wavelet transform

Duan Xiaoyi, Chen Dong, Gaoxianwei, Fan Xiaohong, Jin Jifang
(*Dept. of Electronic Information Engineering*, *Beijing Electronics Science & Technology Institute*, *Beijing* 100070, *China*)

Abstract: In order to improve the efficiency of power analysis attack and reduce the influence of noise, this paper studied the influence of wavelet transform denoising on power attack and the correlation coefficient between Correlation Power Analysis and attack effect. For the purpose of denoiseing the power consumption curve variable, this paper used wavelet method and the wavelet modulus maximum method. The method included the Kalman filter method, the wavelet modulus maximum method and the translation invariant wavelet method. Then the denoised original data are respectively subjected to CPA. Simulation experiments show that compared with the original data, the improved CPA correlation coefficient using the translation invariant wavelet method is 165% higher than using original CPA analysis, 31.4% higher than the Kalman filter method, 26.4% high than the wavelet modulus maximum method. Also the power curve required for successful attack is reduced by 92%. The experimental results show that the improved power analysis using the translation invariant wavelet method has the best effect.

Key words: power analysis; translation invariant Wavelet method; the Wavelet modulus maxima method; crypto chip

0　引言

时间分析技术[1]的提出标志着侧信道信攻击技术诞生，差分功耗分析(differential power analysis，DPA)与简单功耗分析(Simple Power Analysis，SPA)[2]的提出使侧信道攻击的研究进入了一个新的时代。此后各种的攻击方法与防御策略层出不穷，如相关功耗分析（CPA）[3]、多通道分析方法（multi channel analysis，MCA）[4]、高阶差分功耗分析[5]、模板攻击（template attack，TA）[6]等，这些攻击方法的出现不断推动着侧信道攻击与防御对策的不断发展，如加入随机掩码[7,8]加随机噪声[9]等。

研究发现噪声对功耗分析的攻击效率影响很大，文献[10]主要介绍了在含有大量噪声的功耗曲线中如何分析出密钥的方法。功耗信号中的噪声来源通常包括周围电子设备辐射、传输介质与人为加入随机噪声等，而功耗分析的密钥获取是基于采集的功耗信号，真实功耗信号的信噪比很大程度上影响了分析密钥的成功率，所以去除功耗曲线中的噪声能够提高攻击成功率。目前对抑制噪声的方法大多是通过增加功耗曲线样本数量，但实际攻击中功耗曲线样本数量的获取又是有限的，所以无限制的增加使用功耗曲线数量是行不通的。因此，在功耗曲线样本数量有限的条件下，最大程度的减少采样功耗信号中的噪声干扰成为功耗分析研究中的重点。

功耗分析中常见的功耗曲线预处理方法有卡尔曼滤波法[11]、主成分分析法[12]、闵可夫斯基距离法（Minkowski distance）[13]和改进奇异值分解法[14]等。但卡尔曼滤波必须用到无限过去的数据；主成分分析法需要通过获得自相关矩阵来完成特征向量和特征值的求解，且该过程对于正常的计算设备来说涉及到的计算复杂度和存储空间过于庞大，耗时长；闵可夫斯基距离法虽计算简单但没有考虑各个分量的差异化；改进奇异值分解法的难点在于奇异值数目的选取，这些都大大限制了它们在功耗曲线抑制噪声的应用。但小波分析[15]能根据信号局部区域的不同特性变换时频分辨率，即对低频长时信号具有高的频率分辨率和低的时间分辨率；而对高频短时信号具有低的频率分辨率和高的时间分辨率。这种变焦特性使

收稿日期：2018-09-13；**修回日期：**2018-11-13　　基金项目：国家自然科学基金资助项目（NO.61701008）；中央高校基本科研业务费资助项目 (2017LG05，328201801)

作者简介：段晓毅（1979-），男，讲师,博士，主要研究方向为密码芯片安全(duanxiaoyi@besti.edu.cn)；陈东（1995-），女，硕士研究生，主要研究方向为信息安全；高献伟（1970-），男，教授，主要研究方向为信息安全；范晓红（1979-），女，讲师,硕士，主要研究方向为信息安全；靳济方（1972-），女，副教授,硕士，主要研究方向为信息安全.

得小波变换对非平稳信号具有很强的自适应性，所以基于小波分析抑制噪声的效果优异，它能有效分离信号和噪声，提高信噪比。因此本文将基于小波分析中的平移不变量小波法与小波模极大值法[16]应用到功耗曲线的预处理中，以达到提升功耗分析效率的目的。

1　功耗曲线能量模型及功耗分析原理

1.1　功耗曲线能量模型

功耗分析中能被攻击者所利用的能量消耗[17]是来源于该加密设备所处理的数据与执行的操作，而电子噪声分量与恒定分量是实际采集的功耗曲线中不可忽视的两个能量分量。因此对于功耗曲线中的单个采样点的总的能量消耗一般由以上四个分量组成，如公式（1）所示。

$$P_{total}=P_{op}+P_{data}+P_{noise}+P_{const} \tag{1}$$

其中：P_{op}、P_{data}、P_{noise} 与 P_{const} 代表操作分量、数据分量、噪声分量与常量分量且它们相互独立。P_{op}、P_{data}、P_{noise} 是对攻击者来说最重要的信息分量，而 P_{const} 分量不包含任何攻击者能利用的信息，所以与功耗分析无关。且攻击者仅仅能够通过分析 P_{op} 和 P_{data} 来获得密钥信息，但随着噪声分量 P_{noise} 的增大会使攻击变得更加困难。为了进一步明确功耗曲线能量模型中的能量分量，用 P_{exp} 代表攻击者可利用的能量消耗分量；信噪比（SNR）定义为实际采集的信号分量和噪声分量的比。在功耗分析中，信噪比公式如式（2）所示。

$$SNR=\frac{\mathrm{Var}(P_{exp})}{\mathrm{Var}(P_{noise})} \tag{2}$$

$\mathrm{Var}(P_{exp})$ 量化了攻击者可利用的信号造成功耗曲线中点变化的大小，$\mathrm{Var}(P_{noise})$ 则量化了由噪声导致的该点的变化大小，SNR 越高，从噪声中识别出 P_{exp} 就越容易。

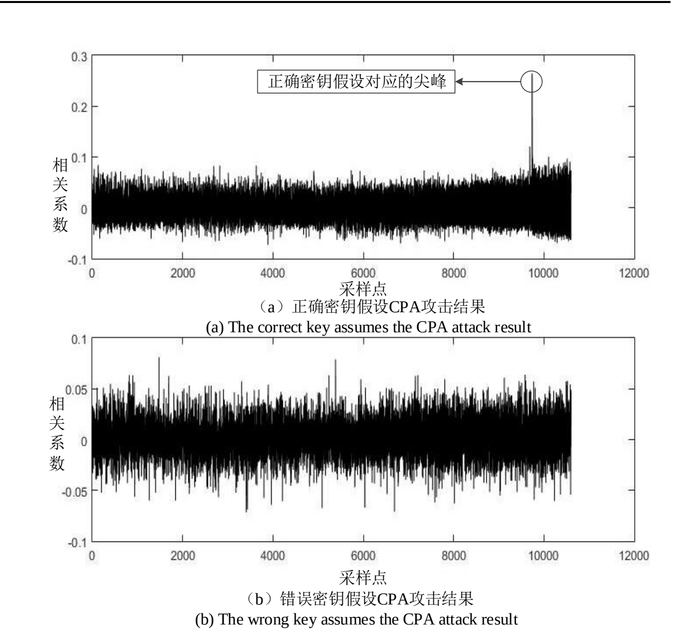
1.2　相关功耗分析原理

密码芯片在运行加密或解密算法的过程中会伴随着能量的消耗。而对于寄存器中的触发器来说所处理的数据与能量消耗的多少是有某种直接联系。这种关系在操作数层面表现为执行指令前后数据的汉明重量或汉明距离，寄存器层面为寄存器中触发器的 0、1 状态的翻转，在 CMOS 门电路层面为负载电容的充放电。所以，能利用执行指令前后数据的汉明重量或汉明距离来分析密码芯片数据处理过程中的能量消耗情况。功耗分析攻击的原理是通过执行加密或解密数据与加密芯片功耗之间的相关性来获取密钥。而相关功耗分析主要是利用实际测量的加密能量消耗与估计的加密中间数据的汉明距离或汉明重量的相关性来进行密钥分析。

在实际工程应用中，首先采集固定密钥加密或解密 N 条明文的功耗曲线，功耗曲线的采样点为 M，于是得到一个 $N\times M$ 维的实测功耗矩阵 T；利用子密钥计算 k_i 来估计出 N 个样本执行同一操作时的汉明重量和汉明距离，于是得到一个 $N\times1$ 维的假设功耗矩阵 $\boldsymbol{H}$；$\boldsymbol{T}_j$ 为实测功耗矩阵 T 的第 j 列，最后计算矩阵 $\boldsymbol{T}_j$ 与矩阵 $\boldsymbol{H}$ 的相关性系数，计算公式如（5）所示。

$$\boldsymbol{\rho}(\boldsymbol{H},\boldsymbol{T}_j)=\frac{\mathrm{E}(\boldsymbol{H}\times\boldsymbol{T}_j)-\mathrm{E}(\boldsymbol{H})\times\mathrm{E}(\boldsymbol{T}_j)}{\sqrt{\mathrm{Var}(\boldsymbol{H})\times\mathrm{Var}(\boldsymbol{T}_j)}} \tag{5}$$

$E(T_j)$ 及 $E(H)$ 分别表示计算它们的数学期望，$Var(T_j)$ 及 $Var(H)$ 分别表示计算各自的协方差，相关系数的结果矩阵 ρ，ρ 越大它们的相关程度越大。正确的子密钥 k_i 对应的相关功耗曲线会出现明显的尖峰如图 1（a）所示，错误的子密钥则无明显尖峰如图 1（b）所示。



（a）正确密钥假设CPA攻击结果
(a) The correct key assumes the CPA attack result

（b）错误密钥假设CPA攻击结果
(b) The wrong key assumes the CPA attack result

图 1　CPA 攻击结果
Fig. 1 Result of CPA

2　相关功耗分析

相关功耗分析是计算假设功耗矩阵 H 和实测功耗矩阵 T 的列之间的线性相关系数，通过出现在相关系数矩阵 ρ 中的尖峰可以分析出被攻击密码芯片所使用过的密钥。但在实际的工程应用中，由于有噪声干扰的存在尤其是人为加入噪声，使得攻击结果的尖峰相关系数相当小的，进而影响到攻击成功率。

根据式（3）对单个采样点的能量消耗进行建模，即用 P_{total} 来表示在采样位置 j 点处加密设备的能量消耗。用矩阵 $\boldsymbol{H}$ 表示预测的能量消耗值。于是得到式（6）。

$$T_j=P_{total} \tag{6}$$

用 P_{total} 替换公式（5）中的 T_j 得式（7）。

$$\boldsymbol{\rho}(\boldsymbol{H},P_{total})=\frac{\mathrm{E}(\boldsymbol{H}\times P_{total})-\mathrm{E}(\boldsymbol{H})\times\mathrm{E}(P_{total})}{\sqrt{\mathrm{Var}(\boldsymbol{H})\times\mathrm{Var}(P_{total})}} \tag{7}$$

用 $\rho(H,P_{total})$ 表示计算二者相关性的大小，将其展开计算如式（8）所示。

$$\rho(H,P_{total})=\rho(H,P_{exp}+P_{sw.noise}+P_{el.noise}+P_{const}) \tag{8}$$

由于 P_{const} 是恒定的常量分量，不会影响到二者的相关系数，而噪声分量 $P_{noise}=P_{sw.noise}+P_{el.noise}$ 在统计上与 P_{exp} 独立，所以继续化简得式（9）。

$$\begin{aligned}\boldsymbol{\rho}(\boldsymbol{H},P_{total})&=\boldsymbol{\rho}(\boldsymbol{H},P_{exp}+P_{sw.noise}+P_{el.noise}+P_{const})\\&=\boldsymbol{\rho}(\boldsymbol{H},P_{exp}+P_{sw.noise}+P_{el.noise})\\&=\boldsymbol{\rho}(\boldsymbol{H},P_{exp}+P_{noise})\end{aligned} \tag{9}$$

将式（9）代入到式（5），得式（10）。

$$\begin{aligned}\boldsymbol{\rho}(\boldsymbol{H},P_{total})&=\frac{\mathrm{E}(\boldsymbol{H}\times(P_{exp}+P_{noise})-\mathrm{E}(\boldsymbol{H})\times\mathrm{E}(P_{exp}+P_{noise})}{\sqrt{\mathrm{Var}(\boldsymbol{H})\times(\mathrm{Var}(P_{exp})+\mathrm{Var}(P_{noise}))}}\\&=\frac{\mathrm{E}(\boldsymbol{H}\times P_{exp}+\boldsymbol{H}\times P_{noise})-\mathrm{E}(\boldsymbol{H})\times(\mathrm{E}(P_{exp})+(P_{noise}))}{\sqrt{\mathrm{Var}(\boldsymbol{H})\times\mathrm{Var}(P_{exp}))}\sqrt{1+\frac{\mathrm{Var}(P_{noise})}{\mathrm{Var}(P_{exp})}}}\\&=\frac{\boldsymbol{\rho}(\boldsymbol{H},P_{exp})}{\sqrt{1+1/SNR}}\end{aligned} \tag{10}$$

式（10）从数学的角度描述了相关系数 ρ 与 SNR 之间的关系。在汉明重量与可利用的能量消耗分量相关系数不变时，

功耗曲线中有用信号的 SNR 变大，$\sqrt{1+1/SNR}$ 变小，则相关系数 ρ 则会变大；反之，SNR 变小，$\sqrt{1+1/SNR}$ 则变大，而相关系数 ρ 则会变小，当小到一定程度时就无法找到相关系数对应的明显尖峰，这使得攻击的难度大大增加，甚至导致攻击失败。

3 小波去噪原理

3.1 小波分析

小波分析是分辨率能自动匹配被分析信号的时频分析方法。在分析低频信号时会选择较长的时间窗口；而分析高频信号时会选择较短的时间窗口。从而完美解决了在实际工程应用中低频信号持续时间长、高频信号持续时间短的问题，所以享有“数学显微镜”的美称。小波分析在模式识别、图像处理、数据压缩、故障诊断、语音识别与信号处理等领域应用广泛。

对于任意的函数 $f(t)\in L^2(R)$ 的连续小波变换为

$$W_f(a,b)=<f,\psi_{a,b}>=|a|^{-1/2}\int_R f(t)\overline{\psi(\frac{t-b}{a})}dt \tag{11}$$

其小波逆变换为

$$f(t)=\frac{1}{C_\psi}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}\frac{1}{a^2}W_f(a,b)\psi(\frac{t-b}{a})dadb \tag{12}$$

其中称 $\psi(t)$ 为一个小波基函数或母小波，如常用的 db11、haar、sym8 与 coif5 等母小波，称 $W_f(a,b)$ 为连续小波变换的结果。

3.2 平移不变量小波去噪

小波阈值去噪凭借其计算过程简单、算法编程易实现与去噪效果优异等优点而被广泛应用在不同领域，但因容易在重构的信号中的奇异点旁出现伪吉布斯现象。而采集的功耗信息信号成分复杂且含有大量的奇异点，所以本文采用平移不变量小波法对功耗曲线进行预处理，该方法能克服小波阈值法导致的伪吉布斯现象。

小波阈值去噪思想：在小波各尺度上将含噪信号进行分解，首先需要本文设置一个阈值，将该阈值与各尺度上的小波系数相比较，大于该阈值的根据一定的规则处理，把小于该阈值的小波系数的置零，最后将剩下的小波系数通过小波逆变换，重构得到去噪后的信号，小波阈值去噪流程如图 2 所示。

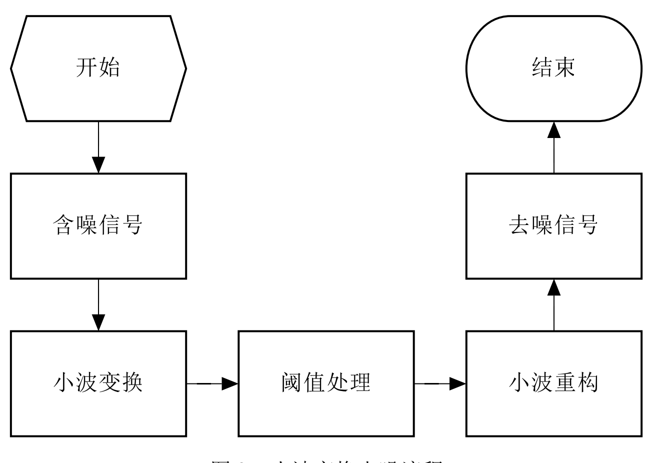


图 2 小波变换去噪流程

Fig. 2 Process of wavelet transform

平移不变量小波法去噪是在小波阈值法去噪的一种改进，其核心思想是：将信号通过循环平移后，其小波系数与原信号的小波系数间无相应的平移关系。即当信号中位于 n_1 位置上的奇异点，其变换结果几乎没有出现伪吉布斯现象；而位于 n_2 位置上的奇异点，则出现了伪吉布斯现象，故可利用变化信号的排列位置，进而改变奇异点的位置来达到抑制振荡现象的产生的目的。即采用人为的移动，将其他位置的奇异点平移到 n_1 位置，达到消除伪吉布斯现象产生的目的，再利用逆向平移，将排列的顺序恢复到与原始信号一样，实现对含噪信号去噪的目的。其中 N 为信号长度，按照以上分析，平移不变量小波去噪步骤是：首先循环平移含噪信号，其平移范围取 N，则是完全平移含噪信号；其次离散小波变换每次循环平移得到的信号，得到不同尺度上的小波分解系数；再通过小波阈值法，对小波系数阈值化处理；小波重构是对剩下的小波系数进行逆变换；求平均后的再逆循环平移，得到去噪信号，如图 3 所示。

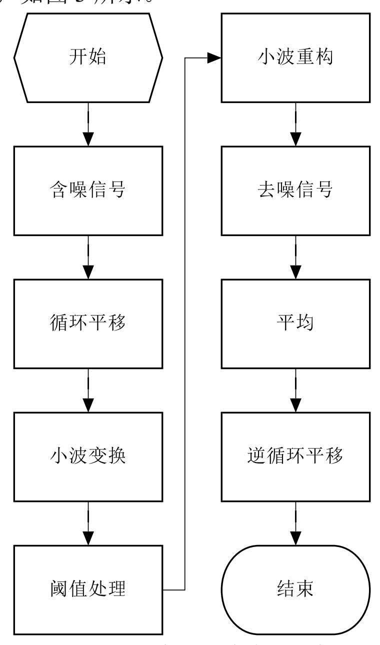


图 3 平移不变量小波法去噪流程

Fig. 3 Process of translation invariant wavelet method

3.3 小波模极大值去噪法

信号的小波变换系数的模极大值反映了此信号的奇异性和峰值性。即噪声的模极大值点会随尺度的增大而减小，信号的模极大值点会随尺度的增大而增大。经过处理后的小波系数利用其在不同分解尺度上剩下的模极大值点来重构信号，这是模极大值去噪的基本思想。

下面通过小波变换来具体研究某点的奇异性。

设小波函数为 $\psi(t)$，若在 t_0 点任意领域内，函数 $f(t)$ 在任意尺度 j 内的小波变换，存在一个常数 k 满足如下关系。

$$|W_{2^j}f(t)|\le k(2^j)^\alpha \tag{13}$$

则函数 $f(t)$ 在 t_0 点处有一致 Lipschitz 指数[18]。将式（13）两边同时取对数可知小波变换的模极大值与信号的 Lipschitz 指数有如下关系。其中 j 为分解尺度，$|W_{2^j}f(x)|$ 表示 $f(x)$ 在 2^j 尺度上 x 轴某一点小波变换的极大值。对上式两边取对数得

$$\log_2|W_{2^j}f(t)|\le\log_2 k+\alpha\cdot j \tag{14}$$

该函数 $f(x)$ 的李氏指数 $\alpha<0$，随尺度的不断增大该函数的小波变换模极大值将减小；若李氏指数 $\alpha>0$，随尺度增大该函数的小波变换模极大值将增大。在奇异性方面信号和噪声有着十分明显的区别，信号的李氏指数是正值，而噪声具有负的李氏指数，所以二者在小波变换的不同尺度上模极大值有明显不同的变化规律，模极大值法则是利用该特点做多次小波变换之后，噪声成分的模极大值点幅值就会被去除或者变得很微弱，所剩余的极值点大部分是由信号产生的，用

剩余的模极大值来重构信号，就获得了去噪后信号，去噪流程如图 4 所示。

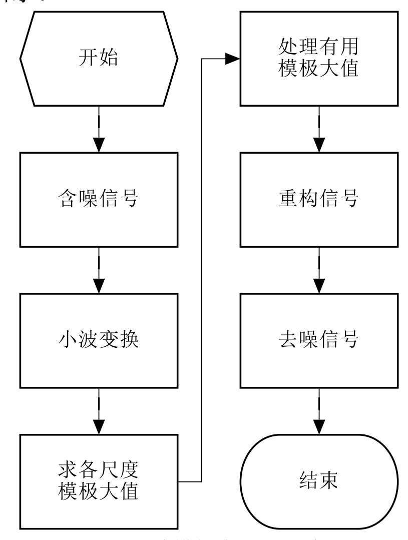


图 4 小波模极大值去噪流程

Fig. 4 Process of Wavelet modulus maxima

4 基于 AES 算法的相关功耗分析

4.1 功耗分析平台与衡量参数

相关功耗分析平台由加密芯片、数据采集、数据处理三部分组成，如图 5 所示。其中加密芯片本文选用 Atmel ATMEGA16A 单片机，时钟频率设置为 4MHz；数据采集部分是由 Tektronix DPO7104 示波器以 50MHz 采样频率采集 10000 条数据样本即（10000 条功耗曲线），每条曲线 25000 个功耗采样点；数据处理是使用 Matlab 软件对功耗曲线分别进行卡尔曼滤波、小波模极大值法与平移不变量法的去噪预处理，再对预处理后的功耗曲线用 VC 执行相关功耗分析，其中本文选取的攻击对象为 128 位 AES 算法第一轮 S 盒输出的字节，最后将攻击的结果用 Matlab 显示出来。

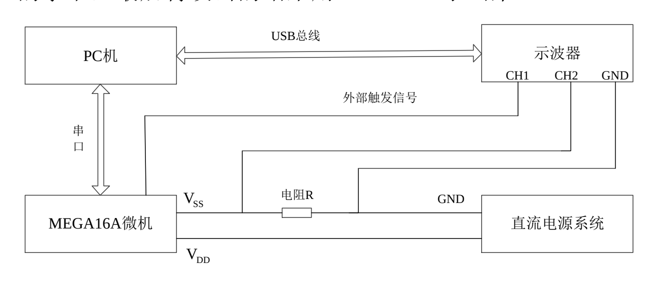
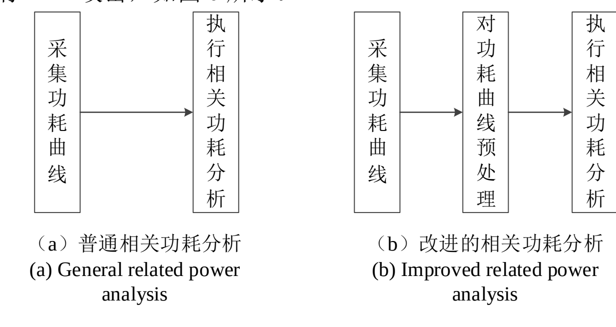


图 5 相关功耗分析平台

Fig. 5 Correlation power analysis platform

普通方案的 CPA 攻击是直接利用功耗曲线来执行分析，而本文改进的相关功耗分析是将功耗曲线进行预处理后再执行 CPA 攻击，如图 6 所示。



（a）普通相关功耗分析 (a) General related power analysis

（b）改进的相关功耗分析 (b) Improved related power analysis

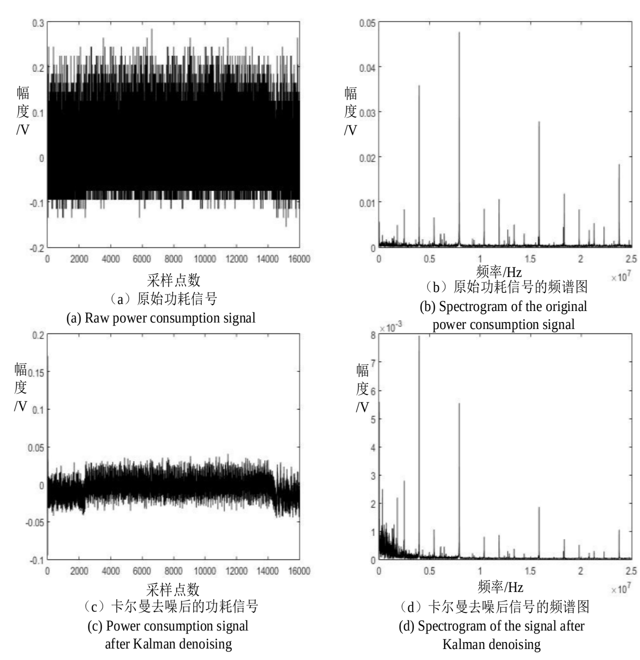
图 6 相关功耗分析方案的改进

Fig. 6 Improvement of correlation power analysis scheme

4.2 功耗曲线的预处理

功耗曲线预处理的目的是为了抑制功耗曲线中不相关的噪声，提高有用信号的 *SNR*，使相关功耗分析结果的相关系数更准确，进而减少分析所需数据量。本文用示波器以 50MHz 采样频率采集固定密钥 10000 条随机明文样本数据，每条功耗曲线有 25000 个功耗采样点。但 AES 算法执行加密操作这一过程只在前 14000 个功耗采样点内，为了减少计算量，本文只对前 16000 个功耗采样点进行处理。

功耗曲线中主要是低频信号成分，为了更好的分析高频信号部分，本文一般对其进行做了去直流处理，剩下的即是功耗曲线中高频信号，最后对其进行傅里叶变换，观察高频信号中的频谱分布。图 7（a）（b）为原始功耗曲线及其频谱图，通过对图 7（a）的直接观察是无法通过简单功耗分析来破解出密钥信息的；从图 7（b）中能直观地看出在 25 MHz 以下高频信号都有分布，这说明采集的功耗数据中包含有较多的高斯白噪声，而几个幅值最大对应的频率是在 16 MHz、8 MHz 与 4 MHz 附近。



（a）原始功耗信号 (a) Raw power consumption signal

（b）原始功耗信号的频谱图 (b) Spectrogram of the original power consumption signal

（c）卡尔曼去噪后的功耗信号 (c) Power consumption signal after Kalman denoising

（d）卡尔曼去噪后信号的频谱图 (d) Spectrogram of the signal after Kalman denoising

图 7 功耗曲线及其频谱图

Fig. 7 Power consumption curve and its spectrogram

下面仔细讨论利用以上三种方法预处理后的功耗曲线波形以及频谱图。图 7（c）（d）为卡尔曼滤波后的功耗曲线及其频谱图，图 7（c）与（a）相比较，功耗曲线的幅值变小，而图 7（d）与（b）相比，高频信号的频率成分主要集中在 8MHz 以内，大多数集中在 4 MHz 以内，8 MHz 以外的频率成分被滤掉。

图 8 是使用小波模极大值法与平移不变量小波法去噪后的功耗曲线及其频谱图。从时域的角度分析去噪后的功耗曲线波形，发现图 8（a）（c）相比图 7（a）（c），功耗采样点变稀疏了，这是因为采用这两种小波去噪法能更好去除信号中的噪声成分，保留有用信号。从频域的角度去比较去噪后功耗数据中的频谱分布情况，图 8（b）与原始功耗数据的频谱图 7（b）相比，使用小波模极大值法去噪后的信号频谱主要集中在 2.5 MHz 以内，此时功耗曲线中的高斯白噪声几乎已近都被滤掉，而图 7（d）中还有大量其他成分的高频噪声，说明卡尔曼滤波并不彻底。图 8（d）与原始功耗数据的频谱图 7（b）相比，使用平移不变量小波法的频谱图中高频成分主要集中在在 2.5 MHz 以内，同时其他频域范围存在的

高频信号与图 7（d）相比已经逼近非常小的值。这只是从频域的角度对三种预处理方法去噪性能进行的粗略分析，最终还需与相关功耗分析相结合，从攻击结果的来衡量抑制噪声的好坏。

因此对预处理方法的性能指标主要从两方面去衡量：相关系数与资源占用，它们分别从攻击效果与攻击效率的角度对预处理方法的有效性进行衡量。

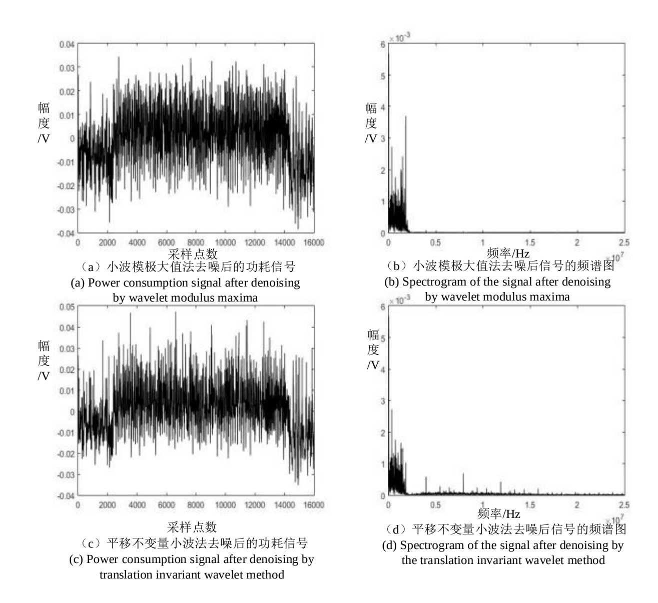


图 8　去噪后功耗曲线及其频谱图

Fig. 8　Power consumption curve and spectrum after denoising

4.3　从攻击效果来衡量

相关功耗分析结果的相关系数大小直接影响攻击结果的成功率。由于功耗曲线中存在的噪声容易导致分析结果出现假峰（ghost peak）。假峰越大对攻击结果的干扰越大，直接影响到正确密钥对应峰值的判别，甚至导致攻击失败。如果能够将功耗数据中的噪声部分较好的去除，提高可利用功耗数据的信噪比，那么正确密钥对应的相关系数峰值与假峰会有明显差别，而当它们的差距进一步拉大时，假峰的干扰就能忽略不计了。所以本文用正确密钥对应的相关系数峰值大小作为衡量预处理方法的去噪性能。使用合适的预处理方法能有效抑制功耗数据中的噪声即减少 $P_{noise}=P_{sw.noise}+P_{el.noise}$，提高 P_{exp} 分量，则假峰消除效果明显，有利于提高相关功耗分析的成功率。

下面从攻击效果的角度对比卡尔曼滤波法、小波模极大值法与平移不变量小波法这三种预处理方法的效果，即使用正确密钥对应的相关系数峰值大小作为抑制噪声效果好坏的标准，因为相关系数越大，SNR 越高。

图 9 是利用 120 条功耗曲线使用正确密钥(第 16 字节密钥）执行相关功耗分析的结果。图 9（a）利用 120 条未经处理的原始功耗曲线执行相关功分析的结果，而图 9（b）~（d）则使用卡尔曼滤波、小波模极大值法与平移不变量小波法去噪预处理后的 120 条功耗曲线执行的相关功耗分析。从图 9（a）中没出现正确密钥所期望的相关系数尖峰，图 9（b）（d）则出现了明显的尖峰，图 9（c）虽然出现尖峰，但是不太明确，对正确判别有较大干扰。由式（3）可知，功耗曲线中有大量的噪声 $P_{sw.noise}$ 和 $P_{el.noise}$ 存在，掩盖了能被利用信号 P_{exp}，即功耗曲线中的 SNR 较小。由式（10）可知 SNR 越小则 $\sqrt{1+1/SNR}$ 越大，$\rho(\boldsymbol{H},P_{exp})$ 就会变小。图 9 实验结果表明用较少的原始功耗曲线执行相关功耗分析是不能猜测出正确密钥信息的。

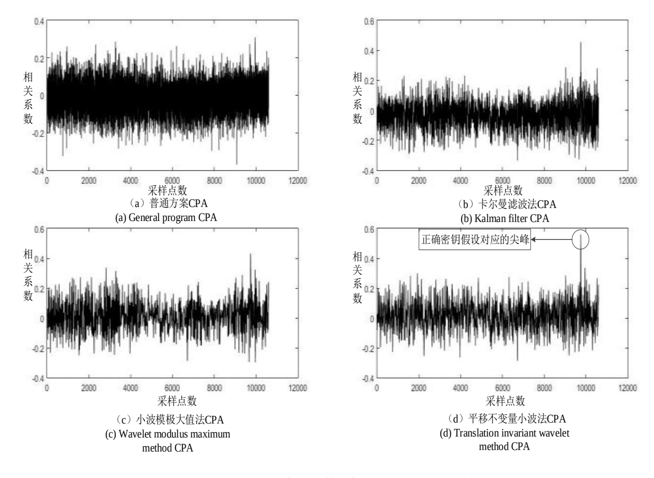


图 9　120 条功耗曲线 CPA 攻击结果

Fig. 9　CPA attack result of 120 power consumption curves

图 10 是利用 400 条功耗曲线使用正确密钥（第 16 字节密钥）执行相关功耗分析的结果。而图 10（a）~（d）中都出现了非常明显的尖峰，说明随着使用功耗曲线数量增多在相关功耗分析中能抑制部分噪声，得到相对明显的攻击结果。此时正确密钥假设对应的尖峰的相关系数图 10（a）为 0.32，图 10（b）为 0.45、图 10（c）为 0.46，图 10（d）为 0.57。平移不变量小波法的攻击结果的相关系数最大，区分度更高，判别干扰小，攻击结果更可靠，所以该方法抑制噪声效果最好的。小波相比模极大值法相关系数提高 23.9%，相比卡尔曼滤波法相关系数提高 26.7%，相比普通方案相关系数提高 78.1%。

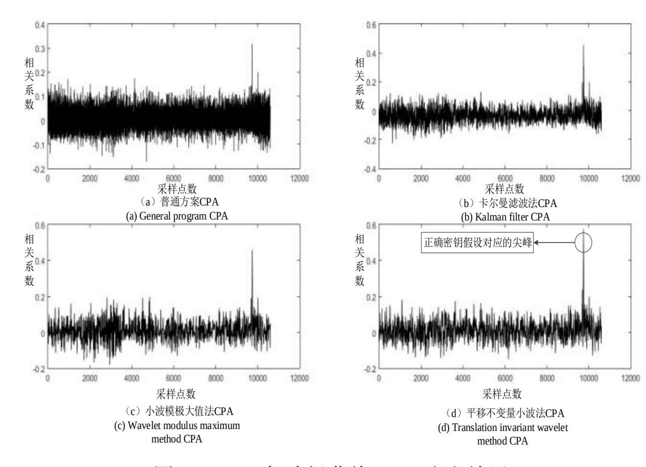


图 10　400 条功耗曲线 CPA 攻击结果

Fig. 10　CPA attack result of 120 power consumption curves

因此从攻击结果可以推出当前条件下使用不同去噪方法的功耗曲线的 SNR 大小：平移不变量小波>小波模极大值法>卡尔曼滤波法。从图 9 与 10 可知噪声干扰对本文的 CPA 攻击影响是十分明显的，除去噪声干扰能够使本文的 CPA 攻击更快和更加准确，这使得利用小波预处理去干扰变得十分有意义。

为了保证实验结果的准确性，表 1 的实验结果是对 5 000 条分别使用这三种预处理方法的功耗曲线执行相关功耗分析得到的，攻击对象为 AES 算法 128 位密钥字节。

使用卡尔曼滤波法、小波模极大值法和小波平移不变量法预处理后功耗曲线的 CPA 攻击效果明显优于普通方案 CPA 攻击效果。小波模极大值法对比卡尔曼滤波预处理后的 CPA 攻击结果，平均每个密钥字节的相关系数比卡尔曼滤波

提高 4.2%，从实验结果来看小波模极大值法比卡尔曼滤波对功耗曲线去噪效果略好。而采用小波平移不变量法预处理后功耗曲线的 CPA 攻击效果明显优于其他预处理技术去噪后的 CPA 攻击，其攻击结果的相关系数相比普通方案的相关系数平均每个密钥字节提高 165%，对比卡尔曼滤波法平均每个密钥字节的相关系数提高 31.4%，对比小波模极大值法平均每个密钥字节的相关系数提高 26.4%。小波平移不变量去噪法适用信号中含有若干不连续点和信噪比较低的情况，所以该方法能够除去功耗信号中不相关的噪声，提高攻击成功率。

表 1 AES16 字节密钥猜测正确时的相关系数

Table 1 Correlation coefficient of AES16 byte key guessing

密钥字节	普通方案	卡尔曼滤波法	小波模极大值法	平移不变量小波法
0	0.32	0.43	0.44	0.51
1	0.15	0.22	0.20	0.27
2	0.11	0.18	0.17	0.22
3	0.13	0.20	0.20	0.25
4	0.14	0.21	0.20	0.27
5	0.11	0.21	0.19	0.25
6	0.08	0.16	0.16	0.21
7	0.07	0.19	0.19	0.25
8	0.07	0.18	0.21	0.26
9	0.08	0.19	0.19	0.24
10	0.06	0.15	0.18	0.22
11	0.05	0.17	0.17	0.23
12	0.06	0.16	0.20	0.25
13	0.06	0.17	0.20	0.25
14	0.04	0.16	0.17	0.21
15	0.11	0.33	0.37	0.46

4.4 从攻击效率来衡量

功耗分析从没有停止追求使用更少的数据得到更加精准的分析结果。而在真实的攻击应用中是不存在完全一样攻击场景下进行多次重复采集的情况，目前大多数攻击技术需要采集大量的功耗数据作为实施攻击的前提条件，所以这个问题的关键在保证分析准确度的情况下尽可能的减少使用功耗曲线样本。所以攻击效率的角度主要是衡量功耗曲线利用率的高低，功耗曲线利用率越高，噪声抑制效果越好。

在使用 CPA 攻击时，为了得到明显的尖峰，需要多少条功耗曲线。图 11 给出了该问题的一个初步答案，该图红色曲线表示正确密钥假设的相关系数，而其他密钥假设的相关系数用黑色来绘制。从图 11 中可以看出，随着功耗曲线数量的增加，正确密钥假设的相关系数从其他的错误密钥假设的相关性中分离出来。

图 11 时使用密钥第 16 字节来执行攻击。图 11~（d）依次是原始功耗曲线与相关系数的关系，利用卡尔曼滤波、小波模极大值法与小波平移不变量法去噪后的功耗曲线与相关系数的关系。从图 11（a）中，正确密钥假设的相关系数随着功耗曲线的增多收敛于 0.08 而其他密钥假设的相关系数收敛于 0.03，当使用 233 条或者更多功耗曲线时，正确的密钥假设导致最高的相关系数出现，因此可以认为一次成功的攻击大约需要 233 条原始功耗曲线。图 11（b）中大约需要 50 条经卡尔曼滤波处理的功耗曲线，图 11（c）中大约需要 54 条经小波模极大值去噪后的功耗曲线，图 11（b）中大约需要 22 条经平移不变量小波法去噪后的功耗曲线。相比使用原始功耗曲线实施 CPA，采用去噪后的功耗曲线执行相关功耗分析会大大提高功耗曲线的利用率。

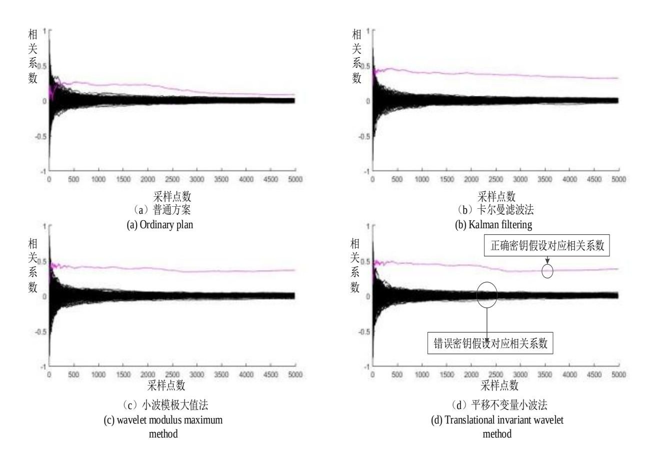


图 11 相关系数与功耗曲线的关系

Fig. 11 Relationship between correlation coefficient and power consumption curve

表 2 相关系数与功耗曲线的数量关系

Table 2 Quantitative relationship between correlation coefficient and power consumption curve

密钥字节	原始数据	卡尔曼滤波法	小波模极大值法	平移不变量小波法
0	90	64	60	64
1	825	356	269	58
2	1214	231	227	253
3	907	414	273	397
4	423	306	160	160
5	403	79	29	10
6	1043	261	39	95
7	5719	123	167	109
8	1049	419	170	77
9	2875	814	465	257
10	6621	419	261	207
11	5095	325	437	247
12	8477	323	269	155
13	3061	83	46	74
14	4498	511	647	736
15	233	50	54	22
sum	42533	4778	3573	2921

表 2 给出的正确密钥的相关系数区分所有 128 为位 AES 算法密钥所需的功耗曲线。从表 2 可知，执行 CPA 攻击分析所有 128 位密钥所需功耗曲线数量最少的是使用平移不变量小波法，只需要 2 921 条，而使用未经去噪的功耗曲线则需要 42 533 条，相比原来减少了 93.1%的功耗曲线。平移变量小波法相比卡尔曼滤波减少了 31.4%的功耗曲线，相比小波模极大值法减少了 26.5%的功耗曲线。由此可知这三种方法功耗曲线利用率最高的是平移不变量小波法，而小波模极大值大法效果略优于卡尔曼滤波法。在实际的工程应用中，由于受到所获取的功耗曲线样本数量的限制，在功耗曲线样本一定的前提条件下，如何高效利用密码设备的功耗曲线来快速破解加密算法就显得尤为重要了。

5 结束语

本文提出使用小波模极大值法与平移不变量小波法对功耗曲线进行去噪预处理。实验结果表明，采用这三种去噪方法对功耗曲线预处理后，相关功耗分析方法的攻击效果与攻击效率都有一定程度的提升。平移不变量小波法抑制噪声干扰的效果最明显，较大程度上抑制假峰的产生，提高了攻击

精度，只需原始功耗曲线数量的 7%就能成功分析出所有 128 位密钥，且每个密钥字节的相关系数相比原来平均提升 165%，所以在相关功耗分析中平移不变量小波法的去噪性能最优。最后通过对比，平移不变量小波法在这三种去噪方法中的效果是最优的。

参考文献：

[1] Kocher P C. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems [C]//Proc of International Cryptology Conference on Advances in Cryptology. 2010: 104-113.

[2] Kocher P, Jaffe J, Jun B, *et al.* Introduction to differential power analysis [J]. Journal of Cryptographic Engineering, 2011, 1 (1): 5-27.

[3] Bottinelli P, Bos J W. Computational aspects of correlation power analysis [J]. Journal of Cryptographic Engineering, 2016, 3 (7): 1-15.

[4] Agrawal D, Rao J R, Rohatgi P. Multi-channel attacks [C]// Proc of International Workshop on Cryptographic Hardware and Embedded Systems. 2003: 2-16.

[5] Zhang Liwei, Ding Aidong A, Fei Yunsi, *et al.* Efficient nonprofiling 2nd-order power analysis on masked devices utilizing multiple leakage points [J]. IEEE Trans on Dependable & Secure Computing, 2017, (99): 1-1.

[6] 李佩之，严迎建，段二朋．DES 密码芯片模板攻击技术研究 [J]．计算机应用与软件，2013，30 (4)：310-312. (Li Peizhi, Yan Yingjian, Duan Erpeng. Research on template attack techniques against DES cryptographic chip [J]. Computer Applications and Software, 2013, 30 (4): 310-312.)

[7] Chari S. A cautionary note regarding evaluation of AES candidates on smart-cards [C]//Proc of Advanced Encryption Standard Candidate Conference. 2010: 133-147.

[8] 李浪，欧雨，邹祎．一种 AES 随机变换掩码方案及抗 DPA 分析 [J]．密码学报，2018，5 (4)：442-454. (Li Lang, OU Yu, Zou Yi. On AES random transform masking scheme against DPA [J]. Journal of Cryptologic Research, 2018, 5 (4): 442-454.)

[9] 徐佩．智能卡 AES 加密模块抗侧信道攻击掩码技术研究与实现 [D]．重庆：重庆大学，2015. (Xu Pei. Research and Implementation with Mask Technology on AES Encryption Module of Smartcard against Side Channel Attack [D]. Chongqin: Chongqin University, 2015.)

[10] Kunihiro N, Takahashi Y. Improved key recovery algorithms from noisy rsa secret keys with analog noise [M]// Topics in Cryptology. Switzerland: Springer International Publishing, 2017.

[11] Souissi Y, Guilley S, Danger J, *et al.* Improvement of power analysis attacks using Kalman filter [C]//Proc of IEEE International Conference on Acoustics, Speech, and Signal Processing.2010: 1778-1781.

[12] Cagli E, Dumas C, Prouff E. Enhancing dimensionality reduction methods for side-channel attacks [M]// Smart Card Research and Advanced Applications. Switzerland: Springer International Publishing, 2015.

[13] Ou Changhai, Wang Zhu, Sun Degang, *et al.* Enhanced correlation power analysis by biasing power traces [M]// Information Security. Switzerland: Springer International Publishing, 2016.

[14] Sun Degang, Zhou Xinping, Wang Zhu, *et al.* POSTER: using improved singular value decomposition to enhance correlation power analysis [M]// Security and Privacy in Communication Networks. Switzerland: Springer International Publishing, 2015.

[15] 李杨．小波去噪方法的研究 [J]．科技视界，2017 (25)：56-56. (Li Yang. Research on wavelet denoising method [J]. Science & Technology Vision, 2017 (25): 56-56.)

[16] 张新鹤．基于小波变换模极大值的信号奇异性检测 [J]．电子制作，2015 (5)：1-3. (Zhang Xinhe. Signal singularity detection based on wavelet transform modulus maxima [J]. Practical Electronics, 2015 (5): 1-3.)

[17] Mangard S, Oswald E, Popp T. Power analysis attacks: Revealing the secrets of smart cards[M]. Springer Science & Business Media, 2008: 61-100.

[18] 华春红，任章，张敏虎．基于自适应阈值估计的模极大值去噪方法 [J]．航天控制，2011, 29 (1): 37-47. (Hua Chunhong, Ren Zhang, Zhang Minhu. The wavelet maxim a denoising based on the adaptive Bayes shrink threshold [J]. Aerospace Control, 2011, 29 (1): 37-47.)